PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-215826
(43)Date of publication of application : 02.08.2002

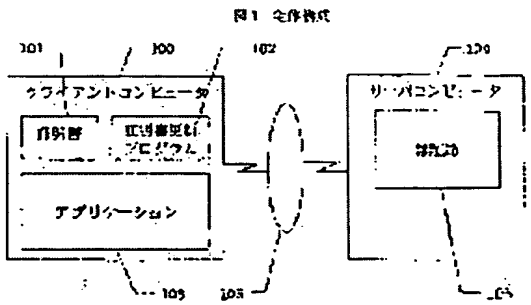
(51)Int.Cl. G06F 17/60
G09C 1/00
H04L 9/32

(21)Application number : 2001-011961
(22)Date of filing : 19.01.2001

(71)Applicant : HITACHI LTD
(72)Inventor : IBA KENICHI
IKEUCHI MANABU
BANDAI KENSUKE

(54) DEVICE AND METHOD FOR AUTOMATIC CERTIFICATE RENEWAL

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a device for automatic certificate renewal which can automatically renew a certificate when the certificate, which has necessary information for renewal itself, will be expired soon or has already expired.
SOLUTION: A certificate renewal program 102, which is connected to a server computer 104 with a certificate authority function and automatically renews the certificate, a storage which stores the certificate, and an application program 103 which uses the certificate are prepared. A client computer 100 is connected to the server computer and requests the server computer to renew the certificate automatically after or at the last days of the expiring date of the certificate. The certificate has a certificate renewal program execution part which executes expiring information and the certificate renewal program. The certificate is connected to the server computer 104 and requests the server computer to renew the certificate automatically after or at the last days of the expiring date of the certificate, besides it receives a renewed certificate and stores it in the storage.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－215826
（P2002－215826A）
(43)公開日　平成14年８月２日(2002.8.2)

(51)Int.Cl.[7]	識別記号	Ｆ Ｉ		テーマコード（参考）
Ｇ０６Ｆ　17/60	１４０	Ｇ０６Ｆ　17/60	１４０	５Ｊ１０４
Ｇ０９Ｃ　1/00	６４０	Ｇ０９Ｃ　1/00	６４０Ｚ	
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７５Ｄ	

審査請求　未請求　請求項の数５　ＯＬ　（全７頁）

(21)出願番号　特願2001－11961(P2001－11961)

(22)出願日　平成13年１月19日(2001.1.19)

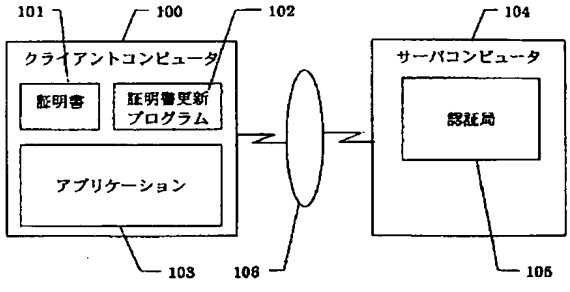
(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　伊庭　健一
神奈川県横浜市戸塚区戸塚町5030番地　株式会社日立製作所ソフトウェア事業部内
(72)発明者　池内　学
神奈川県横浜市戸塚区戸塚町5030番地　株式会社日立製作所ソフトウェア事業部内
(74)代理人　100093492
弁理士　鈴木　市郎　（外１名）

最終頁に続く

(54)【発明の名称】　証明書自動更新装置および方法

(57)【要約】
【課題】証明書の更新作業に必要な情報を証明書自身に持たせて有効期限間近になった場合、あるいは失効した場合に、自動的に証明書を更新することのできる証明書自動更新装置を提供する。
【解決手段】認証局機能を有するサーバコンピュータ１０４に接続して証明書を自動更新する証明書更新プログラム１０２および前記証明書を格納する記憶装置と、前記証明書を利用するアプリケーションプログラム１０３とを備え、前記証明書の有効期限の末期あるいは有効期限の終了後に前記サーバコンピュータに接続して前記サーバコンピュータに前記証明書の自動更新を要求するクライアントコンピュータ１００からなり、前記証明書は有効期限情報および前記証明書更新プログラムを起動する証明書更新プログラム起動部を備え、前記証明書の有効期限の末期あるいは有効期限の終了後に前記サーバコンピュータ１０４に接続して前記サーバコンピュータに前記証明書の自動更新を要求するとともに、更新された証明書を受信して前記記憶装置に格納する。

図１　全体構成



1

【特許請求の範囲】

【請求項１】　認証局機能を有するサーバコンピュータに接続して証明書を自動更新する証明書更新プログラムおよび前記証明書を格納する記憶装置と、

前記証明書を利用するアプリケーションプログラムとを備え、

前記証明書の有効期限の末期あるいは有効期限の終了後に前記サーバコンピュータに接続して前記サーバコンピュータに前記証明書の自動更新を要求するクライアントコンピュータからなり、

前記証明書は有効期限情報および前記証明書更新プログラムを起動する証明書更新プログラム起動部を備えたことを特徴とする証明書自動更新装置。

【請求項２】　請求項１の記載において、前記クライアントコンピュータはリムーバブル媒体に前記証明書情報を格納するリムーバブル媒体駆動装置を備えたことを特徴とする証明書自動更新装置。

【請求項３】　認証局機能を有するサーバコンピュータに接続して証明書を自動更新する証明書更新プログラムおよび前記証明書を格納する記憶装置と、

前記証明書を利用するアプリケーションプログラムとを備え、

前記証明書の有効期限の末期あるいは有効期限の終了後に前記サーバコンピュータに接続して前記サーバコンピュータに前記証明書の自動更新を要求するクライアントコンピュータからなる証明書自動更新方法であって、

前記証明書自動更新方法は、前記証明書の有効期限の末期あるいは有効期限の終了後に前記サーバコンピュータに接続して前記サーバコンピュータに前記証明書の自動更新を要求するステップと、前記証明書更新プログラムを起動するステップと、サーバコンピュータに接続するステップと、サーバコンピュータから証明書の発行を受けるステップと、受けた証明書を記憶装置に蓄積するステップとを含むことを特徴とする証明書自動更新方法。

【請求項４】　クライアントコンピュータに格納した証明書の有効期限の末期あるいは有効期限の終了後に、認証機能を有するサーバコンピュータに接続して該サーバコンピュータに前記証明書の自動更新を要求するステップと、該要求に基づきクライアントコンピュータに格納した証明書更新プログラムを起動するステップと、クライアントコンピュータをサーバコンピュータに接続するステップと、サーバコンピュータから証明書の発行を受けるステップと、受けた証明書を記憶装置に蓄積するステップとを含むプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項５】　認証局機能を有するサーバコンピュータに接続して証明書を自動更新する証明書更新プログラムおよび前記証明書を格納する記憶装置と、

前記証明書を利用するアプリケーションプログラムと認証局機能を有し、少なくとも認証局のアドレス情報を含む証明書を発行するサーバとを備え、

前記クライアントコンピュータは前記証明書の有効期限の末期あるいは有効期限の終了後に前記サーバコンピュータに接続して前記サーバコンピュータに前記証明書の自動更新を要求するとともに、更新された証明書を受信して前記記憶装置に格納することを特徴とする証明書自動更新システム。

2

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は認証局によって発行される公開鍵証明書を自動的に更新することのできる証明書自動更新装置および更新方法に関する。

【０００２】

【従来の技術】近年，インターネット技術が急速に普及し、これに伴い、インターネットあるいはイントラネット上でのデータの盗聴，改ざん，成りすまし等のセキュリティ上の問題が発生してきた。このような問題を解決するため、現在では公開鍵暗号方式を使用したセキュリティ技術が一般的に採用されるようになった。公開鍵暗号方式は、秘密鍵および公開鍵からなる一対の鍵を使用し、前記秘密鍵は他人に漏れないように秘密裡に保管する。一方、公開鍵は他人に公開し、自己に対する暗号文作成等に使用される。このため前記公開鍵とその所有者の関係は第３者によって保証されなければならない。この保証は、通常は前記第３者機関である認証局が公開鍵証明書を発行することにより行われれる。

【０００３】

【発明が解決しようとする課題】前記従来技術においては、前記証明書を使用するユーザーは、認証局から発行された証明書の有効期限が間近になった場合、あるいは失効してしまった場合においては、Ｗｅｂブラウザを介して認証局のホームページにアクセスして，その認証局における証明書の更新手順に従って証明書の更新登録作業を行わなければならない。すなわち、前記証明書の更新作業は、人手を介して行うことから，証明書の更新忘れ、更新手順忘れ等が頻繁に生じていた。

【０００４】ユーザー認証、暗号化、復号化、署名、検定等を行うアプリケーションの中には、証明書の有効期限が間近の場合には、その旨のメッセージを表示してユーザーにその後の証明書の更新作業を促し、さらに、期限切れの場合はエラーメッセージを表示してアプリケーションを停止したり、あるいは証明書を必要とする機能を制限してアプリケーションを立ち上げるものがある。この場合において、証明書を更新するには、一旦アプリケーションを停止して再起動することが必要である。

【０００５】本発明は前記問題点に鑑みてなされたもので、証明書の更新作業に必要な情報を証明書自身に持たせて有効期限間近になった場合、あるいは失効した場合に、自動的に証明書を更新することのできる証明書自動更新装置を提供することにある。

【０００６】
【課題を解決するための手段】本発明は、上記の課題を解決するために次のような手段を採用した。
【０００７】認証局機能を有するサーバコンピュータに接続して証明書を自動更新する証明書更新プログラムおよび前記証明書を格納する記憶装置と、前記証明書を利用するアプリケーションプログラムとを備え、前記証明書の有効期限の末期あるいは有効期限の終了後に前記サーバコンピュータに接続して前記サーバコンピュータに前記証明書の自動更新を要求するクライアントコンピュータからなり、前記証明書は有効期限情報および前記証明書更新プログラムを起動する証明書更新プログラム起動部を備え、前記証明書の有効期限の末期あるいは有効期限の終了後に前記サーバコンピュータに接続して前記サーバコンピュータに前記証明書の自動更新を要求するとともに、更新された証明書を受信して前記記憶装置に格納する。
【０００８】
【発明の実施の形態】以下に本発明の実施形態を図１ないし図５を用いて説明する。図１は、本発明を説明するための全体構成図である。図において、１００は証明書を使用するユーザーの保有するクライアントコンピュータである。１０１はクライアントコンピュータ１００のハードディスク等の記憶装置に格納された証明書である。１０２は認証局に接続し証明書を実際に更新するための証明書更新プログラムである。１０３は証明書１０１を使用して暗号化、署名付与等のセキュリティ技術を使用するアプリケーションである。このアプリケーションは、証明書１０１を使用するアプリケーションであれば、Ｗｅｂブラウザでもユーザーが独自に開発した業務用アプリケーションでもいかなるアプリケーションであってもよい。１０４は証明書１０１を発行する認証局機能を備えたサーバコンピュータである。１０５はサーバコンピュータ１０４上に構築した認証局である。１０６はクライアントコンピュータ１００とサーバコンピュータ１０４を接続している広域ネットワークである。
【０００９】図２は、証明書１０１の格納先がＩＣカードである場合のクライアントの構成例である。２００はＩＣカード内の情報を読み書きするためのクライアントコンピュータ１００に接続したＩＣカードリーダ・ライタである。２０１は証明書１０１を格納したＩＣカードである。本発明によれば，ハードディスクに格納された証明書１０１だけでなく、ＩＣカード２０１に格納した証明書１０１の自動更新も行うことができる。
【００１０】図３は、証明書１０１の格納先がリムーバブル媒体である場合のクライアントの構成例である。３００はリムーバブル媒体内の情報を読み書きするためのクライアントコンピュータ１００に接続されているリムーバブル媒体駆動装置である。３０１は証明書１０１を格納したリムーバブル媒体である。リムーバブル媒体３０１としては、例えばフロッピー（登録商標）ディスク、光磁気ディスクなどがあげられる。本発明によれば、ハードディスクに格納した証明書１０１だけでなく、リムーバブル媒体３０１に格納した証明書１０１の自動更新も行うことができる。
【００１１】図４は、前記認証局により証明書１０１に記録する情報の一例である。４００は証明書１０１の有効期限開始日である。４０１は証明書１０１の有効期限終了日である。４０２は認証局アドレス情報である。この認証局アドレス情報４０２は、認証局１０５への接続仕様に依存し、ＵＲＬあるいはＩＰアドレスとすることができる。４０３は認証局アドレス情報４０２を参照して認証局１０５に接続し、証明書１０１を更新するための証明書更新プログラム名称であり、例えば証明書更新プログラム１０２を指定する。４０４は前記証明書更新プログラム１０２を実際に起動するための証明書更新プログラム起動部である。証明書１０１に対してアプリケーション１０３からアクセスが行われた場合には、この証明書更新プログラム起動部がまず動作する。４０５は前記証明書更新プログラム１０２を起動する手順を示した証明書更新プログラム起動手順である。４０６は証明書の自動更新を有効期限終了日４０１の何日前から行うようにするかを指定した自動更新開始パラメタである。
【００１２】図５は、証明書自動更新装置における全体的なシーケンスの一例を示したものである。ユーザー５００はアプリケーション１０３を起動５０１する。アプリケーション１０３は起動すると、暗号化および署名などを行うのに必要となる証明書１０１にアクセス５０２する。証明書１０１の格納先は、クライアントコンピュータ１００内のハードディスク、ＩＣカード２０１あるいはフロッピーディスク等のリムーバブル媒体３０１のいずれかである。
【００１３】前記証明書１０１の有効期限終了日４０１が現在時刻の間近となっているかまたは失効している場合は、証明書に格納された証明書更新プログラム起動手順４０５に従い証明書更新プログラム名称４０３で示す証明書更新プログラム１０２を起動５０３する。一方、証明書１０１の有効期限終了日４０１が現在時刻の間近になっていなく、かつ失効していない場合はそのままアプリケーション１０３に制御を復帰５０４する。
【００１４】証明書更新プログラム１０２が起動されたら、証明書１０１の認証局アドレス情報４０２に従い認証局１０５にネットワークを介して接続５０５する。続いて証明書更新プログラム１０２は、認証局１０５に対して証明書更新要求５０６を行う。認証局１０５は証明書更新依頼５０６を受け付けると、実際に証明書の更新に必要な情報を得るために、更新手続要求５０７を証明書更新プログラム１０２に対して発行する。更新手続要求５０７を受け取った証明書更新プログラム１０２は、ユーザー５００に対してユーザーから証明書の更新に必

要な情報を得るために、更新手続要求５０８を発行する。

【００１５】更新手続要求５０８を受け取ったユーザー５００は、証明書の更新に必要な情報を入力５０９する。証明書更新プログラム１０２は前記入力５０９された情報を元に更新手続応答５１０を認証局１０５に返す。更新手続応答５１０を受け取った認証局１０５は、更新手続応答５１０に従い、証明書更新プログラム１０２に対して証明書発行５１１を行う。更新後の証明書を受け取った証明書更新プログラム１０２は、ハードディスク、あるいはＩＣカード２０１、フロッピーディスク等のリムーバブル媒体３０１のいづれかに対して証明書格納５１２を行う。その後、証明書更新プログラム１０２は、ユーザー５００に対して証明書の更新手続きが成功したことを示す証明書更新完了５１３を通知し、アプリケーション１０３に制御を復帰５１４する。これにより、ユーザー３００は認証局１０５への接続を意識しなくても、自動的に接続して証明書を更新するので、ユーザは証明書１０１の有効期限終了日４０１に注意を払うことなく業務などを行うアプリケーション１０３を続行することができる。

【００１６】図６は、証明書自動更新処理の流れ図を示したものである。既にアプリケーション１０３は起動されていると仮定している。まず、ステップ６００において、アプリケーション１０３から証明書へのアクセスが行われる。ステップ６０１において、証明書１０１に格納されている証明書更新プログラム起動部４０４が起動される。ステップ６０２において、証明書更新プログラム起動部２０４は、自動更新開始パラメタ読み込み、ステップ６０３において、現在時刻の取得を行う。

【００１７】ステップ６０４において、取得した現在時刻と証明書１０１に格納された有効期限終了日４０１を比較し、証明書の有効期限が失効している場合はステップ６０６に進み、失効していない場合はステップ６０５に進む。ステップ６０５において、有効期限終了日４０１から自動更新開始パラメタ４０６で指定されている日数分を減算して自動更新開始日付を求め、該日付と現在時刻と比較する。自動更新開始日付に到達している場合はステップ６０６に進み、そうでない場合は処理を終了する。ステップ６０６において、証明書更新プログラム名称、起動手順、および認証局アドレスの読み込みを行う。ステップ６０７において、証明書更新プログラム起動部２０４は前記読み込んだ情報を元に証明書更新プログラムの起動を行う。起動された証明書更新プログラム１０２は、ネットワークを介して認証局１０５と接続し、例えば図５のシーケンスで示したシーケンスを経て証明書更新手続きを行う。ステップ６０９において、認証局１０５から更新後の証明書が発行されたら、該更新後の証明書を受け取って記録媒体に格納して処理を終了する。なお、格納先は更新前の証明書が格納されていた

記録媒体とすることができる。

【００１８】図７は、証明書の自動更新を行った後に、更新前の古い証明書を削除するときの流れ図を示したものである。ここでは既に証明書１０１は有効期限間近もしくは失効していて、自動更新が行われる条件とする。まず、ステップ７００において、図５、図６で詳述した証明書自動更新を行い、ステップ７０１において、更新後の証明書を認証局１０５から受け取り、受け取った証明書を格納する。ステップ７０２において、ダイアログメッセージを表示して、ユーザに更新前証明書を削除するかどうか問い合わせる。ユーザが削除する旨の回答を入力したときはステップ７０３に進み、そうでないときは処理を終了する。ステップ７０３において、更新前の証明書を削除する。これにより、古い証明書による記憶媒体のメモリ消費をなくすることができる。

【００１９】図８は、認証局が複数存在し、その各々の認証局から証明書が発行されている場合の全体構成図を示すものである。８００はサーバコンピュータＡである。８０１はサーバコンピュータＡ８００上に構築した認証局Ａである。８０２はサーバコンピュータＢである。８０３はサーバコンピュータＢ８０２上に構築した認証局Ｂである。８０４はクライアントコンピュータ１００のハードディスクに格納された認証局Ａ８０１から発行された証明書である。８０５は同様に認証局Ｂ８０３から発行された証明書である。認証局が複数ある場合においても、前述した単数の場合と同様の手順でそれぞれの認証局から更新後の証明書を受け取ることができる。

【００２０】図９は、図８で示された構成における証明書自動更新処理の流れ図を示すものである。ここでは既に証明書Ａ８０４および証明書Ｂ８０５は有効期限間近もしくは失効していて、自動更新が行われる条件とする。まず、ステップ９００において、アプリケーション１０３から証明書Ａへのアクセスが行われる。ステップ９０１において、証明書更新プログラム起動部４０４は、証明書更新プログラム名称、起動手順、認証局Ａのアドレスの読み込みを行う。ステップ９０２において、読み込んだ情報を元に証明書更新プログラムを起動する。ステップ９０３において、起動した証明書更新プログラム１０２は認証局Ａとの証明書更新手続きを行う。ステップ９０４において、認証局Ａ８０１から更新後の証明書が発行されると、更新後の証明書を受け取り、格納する。

【００２１】ステップ９０５において、アプリケーション１０３から証明書Ｂへのアクセスが行われる。ステップ９０６において、証明書更新プログラム起動部４０４は、証明書更新プログラム名称、起動手順、認証局Ｂのアドレスの読み込みを行う。ステップ９０７において、読み込んだ情報を元に証明書更新プログラムを起動する。ステップ９０８において、起動した証明書更新プロ

グラム１０２は認証局Ｂとの証明書更新手続きを行う。ステップ９０９において、認証局Ｂ８０１から更新後の証明書が発行されると、更新後の証明書を受け取り、格納する。

【００２２】以上により、複数の認証局Ａ８０１及び認証局Ｂ８０３から発行された複数の証明書Ａ８０４及び証明書Ｂ８０５の自動更新が終了する。これにより、認証局が複数でまた、その各々の認証局から発行された証明書を使用する構成においても、証明書の自動更新が可能となる。

【００２３】以上説明したように、証明書の更新作業に必要な情報を証明書自身に持たせて有効期限間近になった場合、あるいは失効した場合に、自動的に認証局に接続して証明書を更新する。したがって、前記証明書を使用してセキュリティを確保するアプリケーションを用いて業務を行うユーザーは、証明書の有効期限や証明書発行機関である認証局への接続を意識しなくても、証明書の有効期限間近や失効した場合において、アプリケーションが証明書にアクセスしたとき、自動的に認証局へ接続し、証明書の更新を行い、そのままアプリケーションに制御を戻すことができる。このため、ユーザーはアプリケーションの停止や再起動などの煩わしさや、証明書を発行してもらうための認証局のアドレスやＵＲＬなどを調べる手間が軽減され、証明書の更新忘れによる業務の停止などを防ぐことができる。さらに、証明書を使用することのできるいかなるアプリケーションに対しても、特に手を加えることなく、前述の自動更新を実装することができる。このためユーザーに対して証明書更新の徹底を図ることが容易になる。

【００２４】

【発明の効果】以上説明したように本発明によれば、証明書の更新作業に必要な情報を証明書自身に持たせて有＊効期限間近になった場合、あるいは失効した場合に、自動的に証明書を更新することのできる証明書自動更新装置を提供することができる。

【図面の簡単な説明】

【図１】本発明を説明するためのの全体構成図である。

【図２】クライアントの構成例を示す図である。

【図３】クライアントの構成例を示す図である。

【図４】証明書に記録する情報の一例を示す図である。

【図５】証明書自動更新処理における全体的なシーケンスの一例を示す図である。

【図６】証明書自動更新処理の流れ図である。

【図７】更新前の証明書を削除するときの流れ図である。

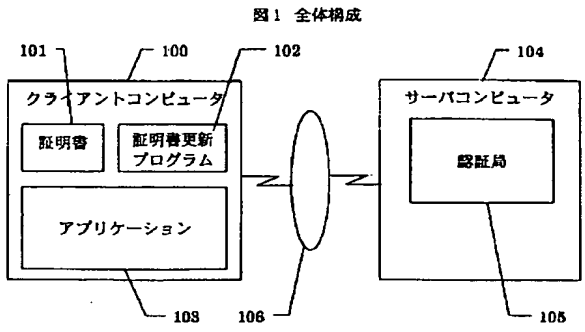
【図８】認証局が複数ある場合の全体構成図である。

【図９】証明書自動更新処理における証明書自動更新処理の流れ図である。

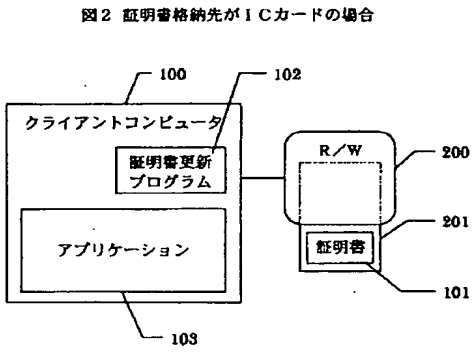
【符号の説明】

１００　クライアントコンピュータ
１０１　証明書
１０２　証明書更新プログラム
１０３　アプリケーション
１０４，８００，８０２　サーバコンピュータ
１０５　認証局
２００　ＩＣカードリーダ・ライタ
２０１　ＩＣカード
３００　リムーバブル媒体駆動装置
３０１　リムーバブル媒体
８０１　認証局Ａ
８０３　認証局Ｂ
８０４　証明書Ａ
８０５　証明書Ｂ

【図１】

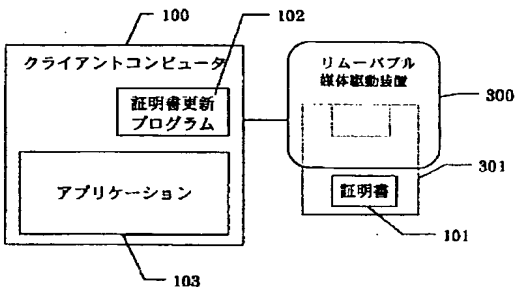


【図２】



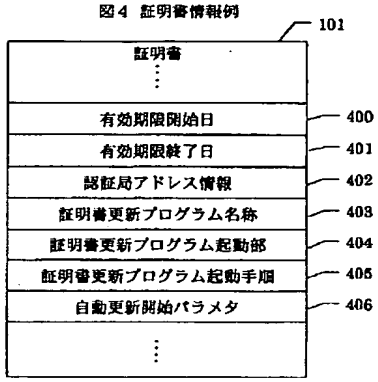
【図３】

図３ 証明書格納先がリムーバブル媒体の場合



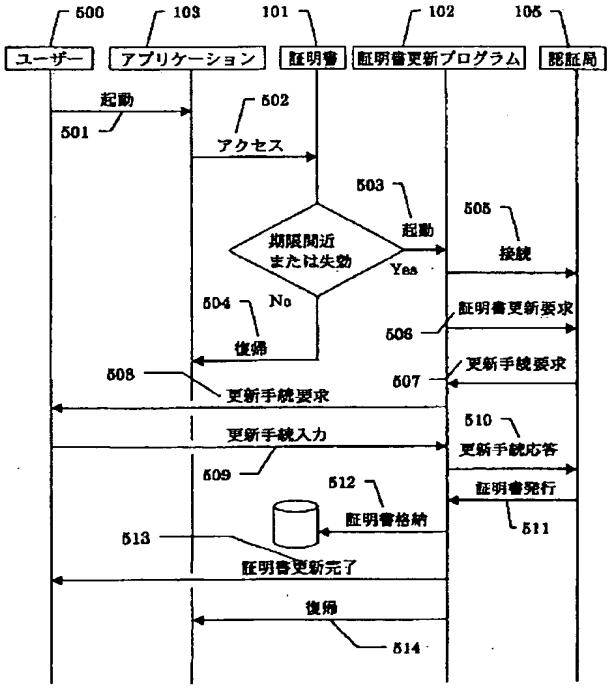
【図４】

図４ 証明書情報例



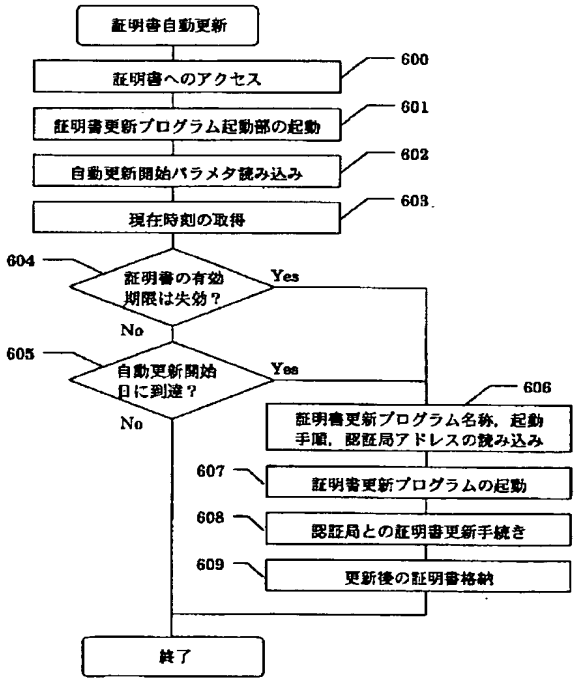
【図５】

図５ 証明書自動更新シーケンス



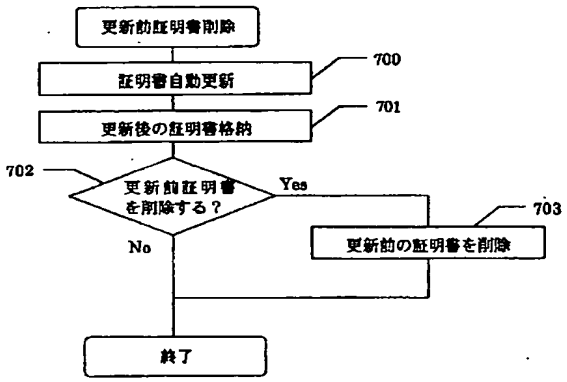
【図６】

図６ 証明書自動更新の流れ図



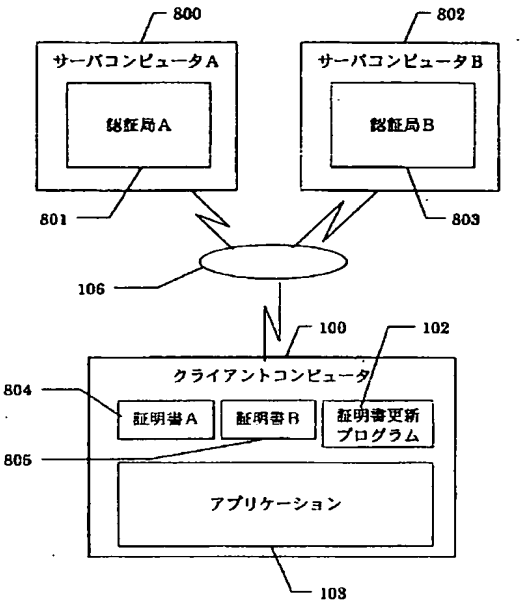
【図７】

図７ 更新前証明書削除の流れ図



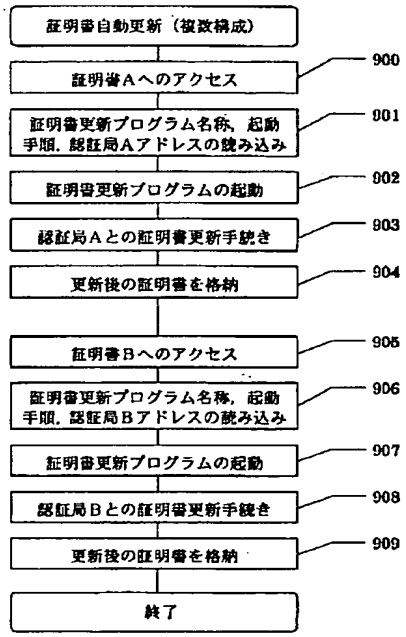
【図８】

図８ 認証局と証明書が複数の構成の場合



【図９】

図９ 認証局と証明書が複数の場合の証明書自動更新の流れ図



フロントページの続き

(72)発明者　萬代　健介
神奈川県横浜市戸塚区戸塚町5030番地　株式会社日立製作所ソフトウェア事業部内

Ｆターム(参考)　5J104 AA12 MA03 NA31 NA32 NA35 PA07